UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,815	01/30/2004	Frederick J. Murphy	1674.00001	5636

86636 7590 08/17/2011

BRUNDIDGE & STANGER, P.C.
2318 MILL ROAD, SUITE 1020
ALEXANDRIA, VA 22314

EXAMINER	
CRIBBS, MALCOLM	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
08/17/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/767,815	MURPHY ET AL.	
	Examiner	Art Unit	
	MALCOLM CRIBBS	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-17,19,22-24,27 and 28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-17,19,22-24,27 and 28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and remarks filed on 06/14/2011 and the supplemental amendment and remarks filed on 08/08/2011.

2. Claims 1-17, 19, 22-24, 27, and 28 are presented for examination.

Response to Arguments

3. **As to the objection of claim 1**, the Applicant states in his remarks "claim 1has been amended to 'determining'," however in view of the supplemental amendment "applying" is recited. Therefore, the objection to claim 1 remains.

4. **As to the USC § 101 rejection to claim 1**, the Applicant states "claim 1 has been amended to overcome this rejection," however claim 1 still recite subject matter that does not necessitate machine implementation which is directed to non-statutory subject matter. Therefore, the rejection to claim 1 remains.

5. Applicant's arguments filed 06/14/2011 and 08/08/2011 have been fully considered but they are not persuasive.

6. It has been argued (page 8 of the remarks 06/14/2011) that "the primary reference relied on, is an object class extension software method and means for IBM's enterprise privacy architecture" while "the present invention, on the other hand, is database agnostic and does not rely on any specific architecture to operate." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., database agnostic and does not rely on any specific architecture to operate) are not

recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

7. It has been argued (page 8 of the remarks 06/14/2011) that "the invention (interpreted as referring to 'neither Alder, Bohrer, nor Cordery teach' for the purposes of examination) also does not access the contents of any database or provide blank forms to any data subject. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., does not access the contents of any database or provide blank forms to any data subject) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. Bohrer in paragraphs [0082] and [0088] discloses:

> [0082] FIG. 5 is a flow diagram of the Request Process, whereby the system receives a data request structure, processes it, and returns a data response structure to the requester. The Profile Responder receives the data request 501. The first step that the responder performs is to authenticate the requester 502. Authentication is the process of guaranteeing that the requester is who they say they are, and can be carried out in several ways, including the use of a userid and password, or a cookie, etc. If the authentication is not successful, then the response is returned with an empty response item list 505. If authentication succeeds, then the data request is passed to the Policy Authorization Engine which retrieves all Authorization Rules of the data subject specified in the request 503. *The data subject is identified from the query in the request, which is applied to the profile database. Once the data subject is identified, all of the authorization rules are retrieved for him/her from the* ***policy database***. If there are no authorization rules for the data subject, the Profile Responder returns a response with an empty response item list. Otherwise, the next step is to examine the Access List of each of these retrieved authorization rules 504. For

each access list, if the requester is not found in the access list, then the authorization is discarded. The requester is in the access list if the requester is either a user in the list or a user in a group which is in the list, or if the access list explicitly authorizes "all" requesters. After this process, if there are no authorization rules left, then the Profile Responder returns a response with an empty response item list. However, if any authorization rules still remain, the Policy Authorization Engine next compares the privacy declarations in the request with the Privacy Preference Rules in the authorization rules for each profile data item name in the request item 506. For each data item name in the query and in the request item list, the Policy Authorization Engine retrieves any privacy preferences from the authorization rules. It then performs the Policy-Preference matching process (see FIG. 6) for each data item. For each application of this matching process, the result is deny 507 or authorize 508, 509, r 510. If the result is deny, then the data item is not included in the list of data items to be returned in the response 511. If the result is authorized, then the data item is included in the response item list 512. Additionally, the authorization rule may require the data subject to be notified 513 or the consent of the data subject be obtained 514. After each data item name is processed, the next data item is retrieved for processing 515. When the entire request list has been processed, the data to be returned is gathered 516, the response structure is constructed and returned to the requester by the Profile Responder 517. If any of the data items have been denied, the Profile Responder may return an empty list to the requester, for more privacy security for the data subject.

[0088] FIG. 7 is a flow diagram of a routine that enables a gather and filtering process carried out to collect data to be returned to a data requester. As described in FIG. 6, the process of matching the privacy policy of the data requester with the authorization rules specified for the requested data by the data subject results in a list of such data items that are to be returned to the data requester. This flow diagram described the various steps that could be potentially involved in the gathering of such data. In step 700, the system examines the list of data items to be returned. *If all the data is available locally on the system 701, the system collects it 702, prepares the reply structure 710 and sends it to the data requester 711. If, however, all data is not available locally, then the system collects whatever data is locally available 703. It then checks if some of the data items have missing values 704. If yes, it contacts the data subject and retrieves the required data items from him/her 705. In step 706, the system determines if the data that is not available locally is available from third parties. If it is available, then the system* ***retrieves the data from the third parties*** *holding the data in step 707.* It then ***filters the data again in step 708 by matching the data returned by the third parties with the request of the data requester and the privacy policies and authorization rules of the data subject.*** This ensures that only that data is returned that is allowed. In step 709, the system authorizes the release of any data that is held by third parties but is

not available for release by the system itself (must be directly requested from the third parties by the data requester). The system then prepares a reply for the data requester 710 by collecting together all the data (locally collected or retrieved from third parties) as well as information about the data authorized to be released by third parties. It then sends this reply to the data requester 711. Thus, by enabling the gather and filter process, a data requester can get data held not only by the system locally but also held by third parties, either via collection by the system itself or directly from third parties after authorization by the system. Since the data subject provides authorization rules describing the privacy preferences and access permissions for all data that is held locally or by third parties, the process ensures that only that data is released, or authorized to be released, for which the data requester is authorized and for which the requesters privacy policies match that of the data subject.

9. Therefore, Bohrer discloses the claimed limitation of querying a database.

10. Alder discloses in paragraphs [0008], and [0041]:

[0008] One advantage of the invention is that it provides a way to enforce privacy policy at the process level ***either manually or via automation***. *For example, a model could be* ***constructed on paper*** *first. Then the instantiated object model could be used as the basis for a design that could be* ***implemented via computer.*** As another example, an information-handling process could be improved by using the model.

[0041] FIG. 3 is a diagram illustrating an example of a method for handling Personally Identifiable Information, along with key terms and concepts, according to the teachings of the present invention. The concepts of an empty form, 306 or 307, for gathering data under a specified policy, and a filled form 304 for representing the gathered data along with the policy, are used when describing data actions. The concept of the empty form, 306 or 307, may be implemented by various techniques for gathering data and specifying policy, such as printed policy statements and email or phone contact. The concept of the filled form 304 may be implemented in any way of capturing input data and storing it, associated with the policy. The main actors in EPA are a data subject 301 (i.e. the person who is described by the PII) and one or more data users, 303 or 304 (e.g. different organizations or individuals). Initially, a data user 303 asks a data subject 301 to release data, 308. ***This done by first sending an empty form 307 that contains fields to fill in, as well as a privacy policy. Then the data subject 301 returns a filled form 302 that contains his or her PII along with the associated policy.*** PII always is associated with policy. Later, a data user 303 may want to send the data to another data user 305. This is called disclosure, 309. A data user 305 sends an empty form 306 including a policy.

> The data user 303 checks to see whether a disclosure to this data user 305 under the given policy is allowed. If so, the data is filled into the empty form 306 and the resulting filled form 304 is sent to the other data user 305. A privacy policy contains a set of rules that are specific to a data user such as 303 or 305. Each rule allows a privacy action on personal data within specified constraints. EPA defines twelve privacy actions. The privacy actions described by the policy rules define the purpose for which data can be utilized and disclosed. Constraints may require consent from the data subject 301 before the action is allowed, or rules may allow consent to be withdrawn. This supports opt-in or opt-out choices for the data subject 301.

11. It has been argued (page 9 of the remarks 06/14/2011) that "all privacy protected date (for purposes of examination interpreted to mean data) is encrypted. This is not the case for Adler." The Examiner would like to note, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., all privacy protected data is encrypted) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner respectfully points out that Cordery, referred to for the *claimed* limitation of encryption/decryption of said data screens, discloses in paragraph [0046] and [0064]:

> [0046] FIG. 2 shows a block diagram of portable communications device 10. Controller 30 receives input from keyboard input circuitry 32 and thumbprint processor 34, which controls thumbprint reader 16 and provides an output representative of a user's thumbprint in a conventional format. *Controller 30 uploads user input, and thumbprint data, to the trusted third party system through encryption/decryption engine 36 and wireless data connection 40. Device 10* ***encrypts and signs data transmitted to the trusted third party*** *system in a conventional manner for communications security, and preferably will have its own code to secure communications. Controller 30 downloads and decrypts* ***encrypted screen data*** *from the trusted third party system through connection 40 and engine 36 and outputs the decrypted data to display 20 through display driver 42.* Preferably wireless data connection 40 communicates through the

cellular telephone network in a conventional manner since this network is believed to provide the broadest geographical range of coverage, but any convenient form of wireless communications can be used in other embodiments of the subject invention. Preferably program code to control devise 10 is stored in read-only memory (ROM) 44 to provide further assurance against unauthorized modification.

12. It has been argued (page 9 of the remarks 06/14/2011) that "The regulations that determine what information is protected are screened for each of the privacy applications, i.e. EU privacy Directive, GLB, HIPAA/HITECH etc. From expert screening, the information categories are distilled, agnostic fields are broadly semantically identified and data field queries are generated. Again, such a feature is not found in Alder." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., The regulations that determine what information is protected are screened for each of the privacy applications) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Objections

13. **Claim 1** is objected to because of the following informalities: In claim 1, the Examiner suggest determining said regulatory compliance ... instead of *applying* as determining more clearly states the intentions of the present invention and coincides with the applicant's specification. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

14. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 1 recites "applying 'legal and contractual' requirements" wherein 'legal and contractual' classifies as new matter as it was not described in the application as originally filed. Appropriate correction is required.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. As to claim 1, the statutory category of the claim is indefinite as it recites as amended "a method and means for..." Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

16. **Claim 1** is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 recites subject matter which has the option of human operations only (*i.e. transforming into non-electronic forms; human completion of data screens; human conversion; and non-electronic feedback*) thus not necessitating machine implementation which is directed to non-statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. **Claims 1 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Publication Number 2003/0004734 to Alder et al. (hereinafter Alder) in view of Publication Number US 2003/0088520 to Bohrer et al. (hereinafter 'Bohrer') in view of Publication Number US 2005/0131839 to Cordery et al. (hereinafter 'Cordery').

18. **As to claims 1 and 13**, Alder teaches a method and means for the secure notification of data subjects in privacy environments defined by directive, law or contract, said method and means comprising the steps: applying legal and contractual requirements for privacy notification of data subjects (*paragraph [0041], [0042], [0086], [0088]*); and transforming said requirements into database field query screens and

forms (*paragraph [0008], [0041], [0042]; wherein the forms of the invention including the privacy policy can be enforced either manually or via automation thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use electronic screens and forms for automation and non-electronic screens and forms for manual enforcement*); human and/or automated completion of said data screens (*paragraph [0008], [0041], [0042]; wherein the forms of the invention including the privacy policy can be enforced either manually or via automation thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use electronic screens and forms for automation and non-electronic screens and forms for manual enforcement*); human and/or automated conversion of said data screens into privacy notification human readable formats (*paragraph [0008], [0042], [0043], [0088]*).

19. Alder does not explicitly teach querying a database for privacy protected information fields contained within said query screens and forms; data subject feedback response methods and means; and conversion of said data subject's feedback responses into database controller notification for deletion, modification or correction of the data subject's information in accordance with said requirements.

20. Bohrer teaches a method of enforcing privacy preferences on exchanges of personal data over a computer network (*Abstract*). Bohrer teaches querying a database for privacy protected information fields contained within said query screens and forms (*paragraph [0082], [0088]*); data subject feedback response methods and means (*paragraph [0036], [0082], [0088]; wherein the data subject's consent can be required in which an email is sent to the data subject in order to indicate in a response whether to*

deny or allow or input missing data for the request); and conversion of said data subject's feedback responses into database controller notification for deletion, modification or correction of the data subject's information in accordance with said requirements (*paragraphs [0033], [0035], [0082], [0088]; wherein the data subject is requested to give consent on allowing or denying access and to modify or correct missing information*).

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of enforcing privacy preferences as taught by Bohrer in the system of Alder in order to allow a data subject to express privacy preference policies for controlling access to their personal data and gives the data subject complete freedom to specify their own their own privacy preference policies for any data exchange request (*paragraph [0017]*).

22. Bohrer teaches a method of enforcing privacy preferences on exchanges of personal data across a network for business transactions such as e-Wallet (*paragraph [0001]-[0003]*). Neither Alder nor Bohrer explicitly teach encryption/decryption of said data screens.

23. Cordery teaches another method of facilitating transactions of business such as e-Wallet (FIG. 3 e-Wallet 10) by transmitting data trough a network between various parties (*Abstract; paragraphs [0001], [0048]*). Cordery teaches encryption/decryption of data screens (*paragraph [0046], [0064], and [0081]*).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of facilitating business transaction as taught by

Cordery in the modified system of Alder and Bohrer in order to provide secure data communications transmitted through a network with confidential or private information (*paragraph [0059], [0064]*).

25. Claims 2, 3, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2003/0065727 to Clarke et al. (hereinafter 'Clarke').

26. **As to claim 2**, neither Alder, Bohrer, nor Cordery teach the electronic privacy notification and feedback response is accomplished via a secure web portal.

27. Clarke teaches a method of providing secured messaging in a communications network environment between customer locations for e-business transactions (*Abstract; paragraphs [0011], [0012]*). Clarke teaches the electronic communication is accomplished via a secure web portal (*paragraph [0057]*).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of communications via a network for business transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a secure communication means in which to transmit private or confidential data (*paragraphs [0012], [0029]*).

29. **As to claims 3 and 23**, neither Alder, Bohrer, nor Cordery teach the electronic privacy notification and feedback response is accomplished via a secure e- mail system.

30. Clarke teaches a method of providing secured messaging in a communications network environment between customer locations for e-business transactions (*Abstract;*

paragraphs [0011], [0012]). Clarke teaches the electronic privacy notification and feedback response is accomplished via a secure e- mail system (*paragraphs [0013], [0016], and [0057]*).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of communications via a network for business transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a secure communication means in which to transmit private or confidential data (*paragraphs [0012], [0029]*).

32. **As to claim 22**, neither Alder, Bohrer, nor Cordery teach the electronic privacy notification and feedback response is accomplished via a secure socket layer web portal.

33. Clarke teaches a method of providing secured messaging in a communications network environment between customer locations for e-business transactions (*Abstract; paragraphs [0011], [0012]*). Clarke teaches the electronic privacy notification and feedback response is accomplished via a secure socket layer web portal (*paragraphs [0040], [0064]*).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of communications via a network for business transactions in the modified system of Alder, Bohrer, and Cordery in order to provide a secure communication means in which to transmit private or confidential data (*paragraphs [0012], [0029]*).

35. Claims 4, 5, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2003/0115468 to Aull et al. (hereinafter 'Aull').

36. **As to claim 4**, Bohrer teaches alerting the data processor of both the data subject's privacy preferences and legal and regulatory compliance requirements relevant to the data subjects privacy preferences (*paragraphs [0035], [0081], [0082], [0088]*); and Cordery teaches the used of communication using digital certificates (*paragraph [0052]*), however neither Bohrer, nor Cordery explicitly teach the electronic privacy notification and feedback response is accomplished using digital certificates comprising: a public or private, commercial or government registration authority; a public or private, commercial or government certificate authority; a digital signature encryption algorithm' a unique non-reputable user electronic identity; issuance of x.509 compliant certificates specifically encoded via extension to alert data processor of the data subjects privacy preferences; and issuance of x.509 standard certificates specifically encoded via extension to alert data processors of legal and regulatory compliance requirements relevant to the data subjects privacy preferences.

37. Aull teaches a method facilitating secure communications through a network by the use of digital certificates (*abstract; paragraphs [0002], [0017]*). Aull teaches a public or private, commercial or government registration authority (*paragraphs [0028], [0031]*); a public or private, commercial or government certificate authority (*paragraphs [0028], [0031]*); a digital signature encryption algorithm (*paragraphs [0006], [0009]*); a unique non-reputable user electronic identity (*table 1; paragraphs [0028], [0031]*); issuance of

x.509 compliant certificates specifically encoded via extension to alert data processor of the data subjects privacy preferences (*paragraph [0026], [0028], [0031]*); and issuance of x.509 standard certificates specifically encoded via extension to alert data processors of legal and regulatory compliance requirements relevant to the data subjects privacy preferences (*paragraph [0026], [0028], [0031]*).

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of facilitating secure communications as taught by Aull in the modified system of Alder, Bohrer, and Cordery in order to verify the identity and credentials of the sender and to restrict access to only those whom are authorized (having the correct key) to receive and view the communication (*paragraph [0031]*).

39. **As to claim 5**, Aull teaches the digital signature algorithm is SHA-1 with DSA (*paragraph [0006], [0009]*).

40. **As to claim 28**, Bohrer teaches the binding of a user's identity and access authorizations to software tokens and challenging the tokens at a remote email server or secure web portal in order to gain access to the users authorized email or web messages (*paragraph [0046]*).

41. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Patent Number US 7,493,497 to Tan, Jr. (hereinafter 'Tan').

42. **As to claim 14**, neither Alder, Bohrer, nor Cordery teach a USB key that containing encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query for said data fields.

43. Tan teaches another method of facilitating secure electronic communications through a network (*abstract; column 1, line 29-42*). Tan teaches a USB key that containing encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to query for said data fields (*column 3, line 51-54; and column 3, line 62 to column 4, line 58*).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of facilitating electronic communications as taught by Tan in the modified system of Alder, Bohrer, and Cordery in order to provide secure communications by validation and authentication of external systems to secure the privacy of electronic data exchange and transactions of the system (*column 1, line 29-42; and column 4, line 59 to column 5, line 3*).

45. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2004/0078599 to Nahum.

46. **As to claim 15**, neither Alder, Bohrer, nor Cordery teach a hardware firewall that contains encryption and processing circuitry, authorized user bound identity information

and volatile and/or non- volatile memory that stores the algorithms used to query said data fields.

47. Nahum teaches a method of securing data stored in a storage accessible over a network (*abstract; paragraph [0014]*). Nahum teaches a hardware firewall that contains encryption and processing circuitry, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said data fields (*paragraph [0086]; wherein it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a firewall as software or hardware based on user desirability*).

48. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of securing data accessible over a network in the modified system of Alder, Bohrer, and Cordery in order to restrict access to the data by unauthorized users thus providing security by keeping the unauthorized user isolated from the storage (paragraph [0086]).

49. **As to claim 16**, neither Alder, Bohrer, nor Cordery teach a software firewall that contains encryption and processing instruction sets, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said data fields.

50. Nahum teaches a method of securing data stored in a storage accessible over a network (*abstract; paragraph [0014]*). Nahum teaches a software firewall that contains encryption and processing instruction sets, authorized user bound identity information and volatile and/or non- volatile memory that stores the algorithms used to query said

data fields (*paragraph [0086]; wherein it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a firewall as software or hardware based on user desirability*).

51. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of securing data accessible over a network in the modified system of Bohrer, and Cordery in order to restrict access to the data by unauthorized users thus providing security by keeping the unauthorized user isolated from the storage (paragraph [0086]).

52. Claims 17 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder, Bohrer in view of Cordery in further view of Applicant's Admitted Prior Art (hereinafter 'AAPA').

53. **As to claim 17**, Bohrer teaches deriving privacy regulatory compliance requirements for the protection of personal data (*paragraphs [0005]-[0007]*), however neither Alder, Bohrer, nor Cordery teach the privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

54. AAPA teaches a method of protecting personal data using privacy policies. AAPA teaches that the European Union Privacy Directive objective was to protect personal data, thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to derive privacy regulatory compliance requirements based on the

European Union Privacy Directive to protect personal data (*Specification page 4, 2nd paragraph of the background of the invention*).

55. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of protecting personal data using privacy polices as taught by AAPA in the modified system of Alder, Bohrer, and Cordery in order to protect personal data from unintended or unknown access by unauthorized users (*Specification page 4, 2nd paragraph of the background of the invention*).

56. **As to claim 19**, Bohrer teaches deriving privacy regulatory compliance requirements for the protection of personal data (*paragraphs [0005]-[0007]*), however neither Alder, Bohrer, nor Cordery the privacy regulatory compliance requirements are derived from the laws, rules and regulations promulgated by The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

57. AAPA teaches a method of protecting personal data using privacy policies. AAPA teaches that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) objective was to protect the confidentiality and privacy of personal data, thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to derive privacy regulatory compliance requirements based on the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect personal data (*Specification page 4, 1st paragraph of the background of the invention*).

58. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of protecting personal data using privacy polices as taught by AAPA in the modified system of Alder, Bohrer, and Cordery in order to

protect personal data from unintended or unknown access by unauthorized users (*Specification page 4, 1st paragraph of the background of the invention*).

59. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in further view of Publication Number US 2005/0132188 to Khin et al. (hereinafter 'Khin').

60. **As to claim 24**, Bohrer teaches receiving feedback from data subjects via email (*paragraph [0036], [0082], [0088]*), however neither Alder, Bohrer, nor Cordery teach the privacy notification and feedback response is accomplished via postal notification.

61. Khin teaches a method of determining and implementing privacy requirements regarding personal information (*abstract; paragraph [0010]*). Khin teaches the privacy notification and feedback response is accomplished via postal notification (*paragraph [0039], [0070]*).

62. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of implementing privacy requirements in the modified system of Alder, Bohrer, and Cordery in order to provide the customer the ability to decide whether their data should be shared in a rare instance in which e-mail or the network is unavailable (*paragraph [0070]*).

63. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Patent Number US 7,218,735 to Coron et al. (hereinafter 'Coron').

64. **As to claim 6**, neither Alder, Bohrer, Cordery, nor Aull teach the digital signature algorithm is an elliptic curve.

65. Coron teaches a method of generating digital signatures for secure communication (abstract). Coron teaches the digital signature algorithm is an elliptic curve (abstract; column 3, line 10-22).

66. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the digital signature generation method as taught by Coron in the modified system of Alder, Bohrer, Cordery, and Aull in order to further provide secure communications while allowing the ability to validate the message originator (abstract; column 3, line 10-22).

67. **As to claim 7**, Coron teaches the elliptic curve is a Koblitz binary curve (abstract; column 3, line 10-22).

68. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Publication Number US 2002/0150241 to Scheidt et al. (hereinafter 'Scheidt').

69. **As to claim 8**, neither Alder, Bohrer, Cordery, nor Aull teach the digital signature algorithm is a block cipher such as Rijndael.

70. Scheidt teaches a method of electronically signing a document to communicated over a network using a digital signature (abstract; paragraph [0011], [0012]). Scheidt teaches the digital signature algorithm is a block cipher such as Rijndael (*paragraph [0084]*).

71. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of electronically signing a document using a digital signature as taught by Scheidt in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide secure communications by providing resistance to counterfeiting of the written signature and the data/document itself being transmitted (paragraph [0011]).

72. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Publication Number US 2004/0098285 to Breslin et al. (hereinafter 'Breslin').

73. **As to claim 9**, Bohrer teaches the data subject's privacy preference is to "opt out" (*paragraphs [0011], [0082]*). Neither Alder, Bohrer, Cordery, nor Aull teach where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

74. Breslin teaches a method of assessing, monitoring, and managing risk management of data privacy (*abstract*). Breslin teaches where encoding the digital certificate to be easily read by visual inspection by distinct color coding (*paragraph [0072]*).

75. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the risk management of privacy data method as taught by Breslin in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide the

user the ability to visually quickly determine the status of the digital certificate (*paragraph [0072]*).

76. **As to claim 10**, Bohrer teaches the data subject's privacy preference is to "opt in" (*paragraphs [0011], [0082]; wherein the data subject consents to allow*). Neither Alder, Bohrer, Cordery, nor Aull teach where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

77. Breslin teaches a method of assessing, monitoring, and managing risk management of data privacy (*abstract*). Breslin teaches where encoding the digital certificate to be easily read by visual inspection by distinct color coding (*paragraph [0072]*).

78. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the risk management of privacy data method as taught by Breslin in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide the user the ability to visually quickly determine the status of the digital certificate (*paragraph [0072]*).

79. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Publication Number US 2003/0035548 to Kwan.

80. **As to claim 11**, neither Alder, Bohrer, Cordery, nor Aull teach including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions.

81. Kwan teaches digital certificates and the recovery of encryption keys (*abstract*). Kwan teaches including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions (*abstract; paragraph [0022], [0023]*).

82. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of digital certificates and recovery of encryption keys as taught by Kwan in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide the ability to allow the archival of the private keys corresponding to their digital certificates to be outside of the control of the Certificate Authority in the event the user needs for any reason the certificate to be recovered (*abstract*).

83. Claims 12 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alder in view of Bohrer in view of Cordery in view of Aull in further view of Tan.

84. **As to claims 12 and 27**, neither Alder, Bohrer, Cordery, nor Aull teach the binding of a users identity and access authorizations to a physical device, such as a USB key, and challenging the key at a remote email server in order to gain access to the users authorized email box and messages.

85. Tan teaches another method of facilitating secure electronic communications through a network (*abstract; column 1, line 29-42*). Tan teaches a USB key that containing encryption and processing circuitry, authorized user bound identity information and volatile and/or non-volatile memory that stores the algorithms used to

query for said data fields (*column 3, line 51-54; and column 3, line 62 to column 4, line 58*).

86. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the method of facilitating electronic communications as taught by Tan in the modified system of Alder, Bohrer, Cordery, and Aull in order to provide secure communications by validation and authentication of external systems to secure the privacy of electronic data exchange and transactions of the system (*column 1, line 29-42; and column 4, line 59 to column 5, line 3*).

Conclusion

87. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

88. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

89. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MALCOLM CRIBBS whose telephone number is (571)270-1566. The examiner can normally be reached on 9-5 m-f.

90. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

91. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MALCOLM CRIBBS/
Examiner
Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432